Automatika

Journal for Control, Measurement, Electronics, Computing and Communications

ISSN: 0005-1144 (Print) 1848-3380 (Online) Journal homepage: https://www.tandfonline.com/loi/taut20

Improved QoS and avoidance of black hole attacks in MANET using trust detection framework

J. Manoranjini, A. Chandrasekar & S. Jothi

To cite this article: J. Manoranjini, A. Chandrasekar & S. Jothi (2019) Improved QoS and avoidance of black hole attacks in MANET using trust detection framework, Automatika, 60:3, 274-284, DOI: 10.1080/00051144.2019.1576965

To link to this article: https://doi.org/10.1080/00051144.2019.1576965

AUTOMATIKA
2019, VOL. 60, NO. 3, 274–284
https://doi.org/10.1080/00051144.2019.1576965

SPECIAL ISSUE: COMPUTATIONAL INTELLIGENCE AND CAPSULE NETWORKS

Improved QoS and avoidance of black hole attacks in MANET using trust detection framework

J. Manoranjini[a], A. Chandrasekar[b] and S. Jothi[b]

[a]Department of Information and Communication Engineering, Anna University, Chennai, India; [b]Department of Computer Science and Engineering, St. Josephs College of Engineering, Chennai, India

ABSTRACT

In recent times, secured routing is a major research in MANETs. The behaviour of malicious nodes in this network increases the risk of threats and induces abnormal operations in MANETs. This affects the security of data transmitted between the nodes in the network. Hence, an effective technique is needed to prevent the abnormal nodes after the process of detection. In this paper, we propose an improved Trust Detection Algorithm to increase the probability of detection and prevention of Black Hole nodes in MANETs. The proposed framework observes the behaviour of each node using various trust metrics that includes the relationship between the sensor nodes, social and service attribute trust and QoS metric trusts. The behaviour of sensor nodes is found through the communication and mobility behaviour of each node. This method avoids the black hole nodes in MANETs, when the routing is carried out with Zone Routing Protocol (ZRP). Hence, the privacy of data is retained using the proposed method. The proposed method is tested in terms of different combinations of with and without trusts. The result shows that the proposed method is effective through various QoS metrics like overall throughput, packet loss, energy consumption, trust level, false acceptance rate and missed detection rate.

ARTICLE HISTORY
Received 30 October 2018
Accepted 24 January 2019

KEYWORDS
Black hole attacks; trust detection algorithm; abnormal nodes detection; Zone routing protocol

1. Introduction

The Mobile Adhoc Network (MANET) is a collection of wireless nodes, where each sensor nodes communicates with each other through access-points. The wireless sensor nodes have the capability of cooperating with other nodes, dynamically configures with other nodes and acts as intermediate nodes to assist in routing the packets between the source and destination node [1]. MANETs are employed widely for applications like personal area network, military and emergency rescue operation [2]. The mobility of wireless nodes varies dynamically within the network, the MANETs are considered as time-variant one. Hence, network security, link failure and quality of service (QoS) are considered as an open challenge [3] in the field of MANETs.

The conventional securing routing protocols fail to compromise the QoS in MANETs. Since most of the security-aware routing techniques are proposed either based on trust or cryptographic, where the former offer reduced overhead than the latter. The computational complexity of trust-based model is 0.9 times lesser than the cryptographic methods [4]. In addition, the authors assumed that all the sensor nodes are trustworthy, hence, the cryptographic models are considered as irrational [5]. Furthermore, the presence of malicious nodes in MANETs is considered as a serious security threat that largely affects the performance of network. The administering such attacks have to be done necessarily at regular time instant to maintain the network performance and to avoid the network getting collapsed.

In order to mitigate these limitations and issues and to improve the performance of routing protocol, the concept of trust management is established for securing the wireless nodes. In MANETs, the trust models [6] monitor the sensor nodes cooperation at the time of forwarding the packet in order to calculate the trustworthiness of sensor nodes. The monitoring operation poses reduced complexity in MANETs subjective to the trust evaluation metrics [7]. The trust method can be utilized for finding the routing path with a definite confidence degree between the sensor nodes. However, this cannot secure the sensor nodes that are subjected to various types of attacks. Furthermore, it limits the network dynamic characteristics and rejects the collection of multi-source information [8].

Hence, in order to improve the cooperation, management and evaluation, the trust model should be considered with various attributes of sensor node trust [9] including honesty and ability, collaboration [10], reputation, level of cooperation. This helps in establishing, monitoring and managing trust in distributed systems [11], which enhances the monitoring ability and cooperation among sensor nodes with improved

CONTACT J. Manoranjini manoranjini.phd@gmail.com Anna University, Chennai, Tamilnadu 600025, India

trustworthiness [12]. Thus, multiple trust factor and QoS routing metrics are used, while managing routing in MANETs with trust-based cooperation.

The trust behaviour available in distributed systems is considered a degree of subjective confidence [13] of a sensor node behaviour [14]. The evaluating sensor node has the ability to assess the evaluated sensor node [15] behaviour based on the direct trust level. Depending on past interactions of the evaluated node, any sensor node can recommend them as recommending node [13]. The recommended behaviour is considered to be random since it decays or rises at any time instant. Hence, the sensor node behaviour is considered to be more similar to human behaviour, where the interactions between any two nodes are nil and on other hand, such sensor node acquaints with other sensor node in case of better interaction based on trust level developed over a particular time instant [16]. Conversely, such type of interaction between the sensor nodes show misbehaviour due to its non-participation of sensor nodes in routing that takes into consideration including dishonesty and energy constraints. Hence, the basic functionality of network is greatly affected.

This paper present a framework that encompasses various trust metrics including trust relationship between the nodes, social trust, service attribute trust and trust due to QoS attributes for mitigating the malicious wormhole node behaviour in MANETs. The trust relationship between the nodes is of direct, indirect or mutual trust, the QoS attribute trust is estimated in terms of trust between the sensor node and cluster head, between the cluster heads, between the clusters. The evolution of trust is carried out in all possible ways in a network and no additional metrics are required to evaluate the method. This helps to estimate the trustworthy communication links to carry out the transmission between the sensor nodes without the presence of blackhole nodes.

The outline of the paper is mentioned below: Section 2 provides the related works. Section 3 discusses the proposed trust models. Section 4 deals with the performance metrics required to test the proposed model. Section 5 evaluates the trust model with various metrics. Section 6 concludes the paper.

2. Related works

In MANETs, the successful transmission of packets between the sensor nodes is ensured by Trust and reputation management, which considers cooperation between the sensor nodes to perform the fundamental activities of the network. Several researchers have identified the significance of using trust concept for analyzing the behavioural relationships between the sensor nodes [17]. The trust model helps in improving the integrity of services and strengthen the benefits offered by MANETs.

In recent years, various trust-based models have been identified in MANETs for enhancing its security that aims at authorizing the sensor nodes to evaluate the behaviour of its neighbourhood sensor nodes through direct or indirect manner [18]. The conventional trust model operates on predicting the trustworthiness of sensor nodes and quantifying it based on an evaluation metric. However, the evaluation metric used is a simple measure that does not adequately evaluate the trustworthiness of sensor nodes due to its aggressive dynamic behaviour in a certain environment [19]. Hence, the necessity of various metrics is used for evaluating the trustworthiness of sensor nodes. However, this is still a challenging problem due to the use of a certain metric including link quality, selfishness of sensor nodes, varying infrastructure, limited resources, malicious intent and sensor node failure. The use of these metrics for measuring the trustworthiness of sensor nodes makes the measurement to be difficult due to extremely noisy and overstated measurements.

We overviewed various trust models in various applications like Web Services [20, 21], Cloud Service [22–24], peer-to-peer (P2P) systems [25, 26], Internet of Things [27], Wireless Sensor Networks [28, 29] and heterogeneous environment [30] and MANET [31].

In web services, the author of [20] and [21] has utilized QoS attribute (users' preferences and ratings [20], and Response time, Throughput, Availability, Reliability, Latency and cost [21]) to compute the trust value. The dependencies of these metrics are determined based on the outcomes and correlations of multiple QoS metrics. The QoS metrics extracts the preferences of the users to achieve the required task. These preferences scores are integrated with the trust value of QoS metrics for monitoring the network.

Meanwhile, in cloud services, the technique for QoS trust computation [22] looks similar to the QoS trust model of the method in [20], where the model is designed based on user preferences. However, the QoS attribute of [22] uses 10 QoS metrics that varies from the one used in [20]. The authors in [23] used multiple QoS attributes from the field of services computing to predict the trustworthiness. Similar model of [23] in cloud services is seen in [24] that uses various other QoS metrics Response time, availability, number of processes and CPU and physical memory usage.

In IoTs, the trust-based technique in [27] used limited power, storage capabilities, communication, computing, trust, mobility, time consumption, trustworthiness of service provider, scalability and semantic awareness. These metrics are used for finding the trustworthy services in decentralized semantics-based service discovery framework.

In peer-to-peer (P2P) systems, the authors in [25] consider the QoS from a peer as a probabilistic rating that includes average and group reliability, average

credibility and reputation as its QoS metrics. Likewise, the authors in [26] used longevity of the network as its QoS metrics. Both these methods use QoS metrics to evaluate the trust between the nodes in the network. The reputation and behaviour of nodes and user opinions are used for computing the trust.

In heterogeneous environment, the author [30] considers availability, reliability, cost time and response time as its QoS metrics to improve the trustworthy stigmergic service in decentralized environments. This method adapts actively to the dynamic changes and trust fluctuations with potential emergence and degradation of trust ratings.

In Wireless Sensor Networks, the author [28] uses social and QoS behaviour to yield status of the sensor node. This is used to validate the protocol by comparing subjective trust and objective trust. Intimacy, honesty, energy and unselfishness are used as QoS metrics and trust-based geographic routing and intrusion detection are used for detecting the efficiency of the method. The authors in [29] proposed QoS trust estimation model based on social network analysis in order to enable the measurement the QoS of neighbouring node behaviour with the help of a sensor node. The QoS metrics like node, computing, storage, communication, service level, estimation from other nodes are used as QoS metrics for evaluation. This value is used for routing the data packets securely from the source to destination nodes.

In MANETs, the author in [31] used three model that includes QoS metrics measurement, modelling of trust level based on QoS metrics and discovering the routing path. This method uses energy, delay, link lifetime, distance and trust as its QoS metrics to calculate the fitness level.

The disadvantages we found from the existing techniques is given below:

- If a model considers QoS and social attributes, the time varying and energy attributes are not considered. It is referred that there is a shortage of QoS attributes to integrate with the trust model. This leads to poor computation of trust value that does not provide the full trustworthiness of the service.
- In various applications, the trustworthy models incur extra overload to offer considerable security measures for trust services or trust between the nodes.
- The proposed trust model is of transitive type and it does not give a clear picture of how realistic the transitivity model works in association with trust management system.
- Various applications (refer Section 1) use partial social trust relationship and network requirement during the evaluation of trustworthiness of a service or between the nodes.
- During the evaluation of trust between the sensor nodes in the network, the social network properties are often omitted.

It is very apparent from the discussions that estimating the trust with multiple factors including social trust and network properties is still a challenging and an open problem. Since, most of the techniques fail to consider the mobility issues, social relationship, malicious node behaviour and overall QoS requirement. The consideration of sensor node behaviour with QoS requirement has to be addressed necessarily to avoid conflicts. These factors lead makes the trust model unsuitable for MANETs. These issues can be addressed using realistic trust model that deals with heterogeneity, scalability, social relationship and mobility.

3. Proposed trust model for detecting the blackholes in MANETs

In MANETs, blackhole detection is regarded as a major aim in this paper and the detection is carried out based on the status of sensor nodes in clusters. The presence of blackhole nodes in the network tends to increase the packet drops in the network that affects the overall quality of MANETs with reduced throughput. The malicious sensor nodes further increase the bandwidth occupancy and excessive resource consumption between the sensor nodes. The blackhole attack occurs due to data packet drop, route request packet drop and route request change. The trust relationship between any two sensor nodes that exist as direct, indirect or mutual trust between them. The other trust metrics proposed for the given study includes social trust, service trust and QoS trust. These trust metrics is stated in the following section:

3.1. Direct trust

The direct trust model estimates the cooperation, communication and association between the sensor nodes to a certain degree in the network. This establishes the extent of trust relationship between any two sensor nodes. The direct trust relationship between the sensor nodes displays the idea of subjective actions that estimates the direct trust degree. The direct trust degree is analyzed using connection strength and similarity relationship between the sensor nodes. The following definitions show the analysis of direct trust relationship.

Definition 3.1: The connection strength between any two adjacent sensor nodes finds the direct trust and the estimation of direct trust degree is given by

$$d_r(u, v) = \frac{w(u, v)}{w(u)}, \text{ where } d_r(u, v) \in (0, 1], \qquad (1)$$

where $d(u,v)$ is the direct trust degree between adjacent sensor nodes u and v. $w(u,v)$ is the degree of strength between adjacent sensor nodes u and v or it provides the collaborative association between the sensor nodes. $w(u)$ is the overall connection strength between the sensor nodes u and v, which are at neighbourhood distance. The Definition 1 leads to the existence of sensor nodes homogeneity or correlation in the network.

The similarity between adjacent sensor nodes is calculated by determining the total number of neighbour hood sensor nodes between any two sensor nodes. If the similarity between the sensor nodes is high, the nodes lying in neighbourhood overlaps with other sensor nodes at a greater extent. The current transmitting node avoids similarity with other nodes in order to reduce the total number of overlaps with other sensor nodes.

Definition 3.2: The similarity between any two adjacent sensor nodes finds the direct trust and the estimation of direct trust similarity. The estimation is given by the following expression

$$d_s(u,v) = \sum_{t \in N(u) \in N(v)} (I(t))^{-1}, \tag{2}$$

where $d_s(u,v)$ is the direct trust similarity degree between adjacent sensor nodes u and v. $N(u)$ and $N(v)$ is the neighbouring sensor node u and v that finds the node similarity. $I(t)$ is the penetration degree of t between u and v.

From the definitions 2, the direct trust degree between adjacent sensor nodes u and v is given by the following expression

$$d(u,v) = d_r(u,v) + d_s(u,v). \tag{3}$$

3.2. Indirect trust

The data packet transmission between the sensor nodes points out the indirect trust. The non-adjacent sensor nodes, i.e. intermediate sensor nodes in the network leads to the existence of indirect connections. This points out the indirect trust relationship between the non-adjacent sensor nodes, where direct trust relationship between the adjacent sensor nodes is used for the computation process. The data packet transmission between source and destination sensor nodes can either takes place in direct or in multi-paths. Thus, the below definitions gives the indirect trust between direct or in multi-paths.

Definition 3.3: The transmission of data packet takes place via single path between a non-adjacent source node (u) and a non-adjacent target node (v) and this creates an indirect trust relationship between these two sensor nodes, which is given by

$$i_s(u,v) = \begin{cases} mt \dfrac{d_{\max} - d_{u,v} + 1}{d_{\max}} & \text{if } d_{u,v} \le d_{\max}, \\ 0 & \text{if } d_{u,v} > d_{\max}, \end{cases} \tag{4}$$

where, the intermediate route length is given by $mt = \min(d(u,\ u_1),\ \mathrm{d}(u_1,u_2),\ \ldots\ \mathrm{d}(u_n,v))$ and d_{max} is the trust between the sensor nodes with maximum distance.

The indirect trust relationship is used to find the approachable communication path between the two non-adjacent sensor nodes u and v.

The observation made from the indirect trust is that as the distance increases, the integrity between the sensor nodes reduces and simultaneously the transmission accuracy is reduced.

Definition 3.4: A non-approachable or indirect path exists between any non-adjacent source (u) and target node (v) and the trust exist between these two sensor nodes is referred as indirect trust with multi-path. The draining of maximal trust value takes place when this type of trust is estimated, which is given by

$$i_m(u,v) = \max_{paths(u,v)} \{i_s(u,v)\} \tag{5}$$

where $i_m(u,v)$ is the indirect trust degree between the non-adjacent sensor nodes. The intermediate path between the sensor nodes is calculated using $paths(u,v)$. Therefore, the degree of trust in the indirect multipath model is estimated by

$$t(u,v) = \begin{cases} d(u,v) & \text{if nodes are adjacent,} \\ i_m(u,v) & \text{else,} \end{cases} \tag{6}$$

3.3. Mutual trust

The value of trust between a pair of sensor nodes is not always similar and hence a directional property is required to justify the trust relationship between the nodes, when $t(u,v) \neq t(v,u)$. The malicious sensor nodes, in addition, may not send message response to the source node. This leads to disparity in trust level between the adjacent sensor nodes. Hence, it creates a negative influence on the detection accuracy that uses trust-based model.

Definition 3.5: The mutual trust between any two adjacent sensor nodes u and v is represented in terms of a non-directional reciprocal trust. Hence the mutual trust between the sensor nodes, when the value of trust relationship $T(u,v) = \{\text{trust}(u,v), \text{trust}(v,u)\}$ is given by

the following expression.

$$m(u,v) = \begin{cases} \min(T(u,v)) & \text{if } \min(T(u,v)) \geq \chi \\ 0 & \text{else} \end{cases} \tag{7}$$

where χ is the trust tolerance degree for controlling the minimum allowed trust level in MANETs. The mutual trust model resolves well the malicious sensor node behaviour in the network and the limitations are reduced during the trust level computation and leads to increased accuracy.

The trust between the sensor nodes u and v in MANETs is estimated using direct, indirect or mutual trust models. The trust value $t(u,v)$ is estimated either through direct or through indirect trust i.e. when the two sensor nodes are not adjacent to each other, the indirect trust model $d(u,v)$ is used. If the two sensor nodes are adjacent to each other, the direct trust model $i(u,v)$ is used. Similarly, the computation of mutual trust $m(v,u)$ is carried out if the trust values between the two sensor nodes are not same. In the end, the mutual trust between the sensor nodes is calculated after comparing the trust levels $t(u,v)$ and $t(v,u)$.

In addition, the proposed system estimates the trust level of sensor node in terms of social trust and QoS trust between the sensor nodes u and v.

3.4. Service attribute trust and social trust

The relationship between the sensor nodes reflects its social interaction and this establishes the degree of trust between them. The relationship between the sensor nodes for calculating the service attribute and social trust is estimated through graph theory that estimates the trust w.r.t the sensor node relationships. Consider a sensor nodes in the network that moves randomly and we use random walk process to transfer the data between the sensor nodes u and v. Hence, the correlation between them is described in terms of a Markov Chain. As the degree of trust between the sensor nodes is high, the communication between them is in increasing trend. Hence, the social relationship between the sensor nodes is strengthened as the communication probability between the sensor nodes increases. Thus the tendency of data communication between the sensor nodes is evaluated for measuring the degree of trust between the sensor nodes, which is given by

$$w(u,v) = \begin{cases} \dfrac{1}{T(u,v)} & \text{if } v \in N_p(v), \\ 0 & \text{otherwise,} \end{cases} \tag{8}$$

where $T(u,v)$ is the degree of trust between the sensor node, which can either be direct, indirect or mutual trust, $N_p(u)$ is the connection between the neighbourhood sensor nodes of u in relation with the u itself. However, the understanding between the sensor nodes is not equal, i.e. the mutual trust between them is not the same. Therefore, the various edge weight (E) denoted by $ss(u,v)$ represents the social strength of connection between the nodes, which is given by the following expression

$$w(u,v) = \begin{cases} \dfrac{ss(u,v)}{\sum_{(u,v)\in E} ss(u,v)} & \text{if } v \in N_p(v), \\ 0 & \text{otherwise,} \end{cases} \tag{9}$$

The strength of social connection increases when the sensor nodes communicate for a longer distance. Hence, it is necessary to calculate how longer the communication between the sensor nodes exists. This is estimated as a function of social strength and an assumption is considered, where communication between the sensor nodes does not with a stranger node.

$$ss(u,v) = f(I(u,v), D(u,v), C(u,v)), \tag{10}$$

where $D(u,v)$ is the duration of communication or the time duration when the sensor node u contacts v, where the time interval of sensor v may overlap the time interval of u.

$I(u,v)$ is the interval of communication between the nodes or the time duration when the sensor node u contacts v from their last contacted time of $D(u,v)$ and $C(u,v)$ is the context of communication that represents the communication scenario based on its location and time that indirectly supports the social strength.

Furthermore, we measure the social attribute vector using a social attribute vector a_u of a sensor node of u. The sensor nodes participation in MANETs makes the communication between the sensor nodes to be subjective to a greater extent. In other words, the establishment of communication between the sensor nodes is not genuine and it depends entirely on the degree of trust between the sensor nodes and whether the demand for communication between them lies on a specific attribute. Such importance in the trust degree for a sensor node attribute, the probability of communication behaviour between the sensor nodes is not similar to a specific attribute. Hence, the communication between is categorized as importance in social attribute degree, which is expressed as

$$e(u,a_v) = \frac{1 + |N_a(u)| \cdot \sum_{u_m \in N_p(u)} w(u,u_m) \cdot g(u_m,a_v)}{|N_a(u)| + (1 + |N_p(u)|)}, \tag{11}$$

where

$$g(u_m,a_v) = \begin{cases} 1 & A(a_v) = 1, \\ 0 & \text{otherwise,} \end{cases} \tag{12}$$

$|N_p(u)|$ is the set of users connected with the edge u; $|N_a(u)|$ is the set of users connected with a social attribute vector;u_m is the total number of users relied

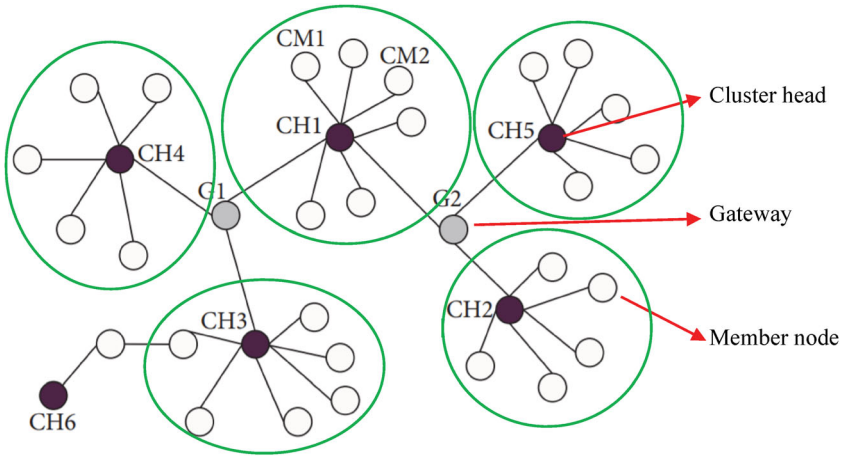

Figure 1. Illustration of zones in MANETs.

on sending the information via a sensor node u and $w(u,u_m)$ is the demand probability of a certain attribute.

Equation (11) shows the trust degree of a sensor node attribute affected by both the malicious node and due to the distribution of these attributes between its neighbouring nodes.

3.5. QoS trust

The ZRP [32] uses a one-hop clustering algorithm that splits the network into zones led by reliable leaders that are mostly static and have plentiful battery resources. The measurements led by this protocol is used for the measurement of QoS Trust between any two sensor nodes, say u and v. This protocol divides the entire network into zones (shown in Figure 1) that makes the calculation of QoS trust easier between the sensor nodes and it does not require the calculation of trust for longer distances. Furthermore, effective communication between the zones is taken into the account of measuring the trust between the nodes using QoS metrics.

The QoS trust metrics are used for detecting the detection of black holes based on the trust level between each sensor nodes, which is estimated using various trust that includes: negative trust, capacity trust, ability trust, safety trust, experience trust and security trust. Certain QoS metrics like rate of transmission, past communication history and number of connections acquired is used for QoS trust estimation. The computation is carried out between neighbourhood sensor nodes. The trust computation between the sensor nodes is given below.

3.5.1. Model assumption

- Case 1: The degree of trust $T(u,v)$ between the sensor nodes u and v can be referred to as a constant function that lies within a time interval (τ).
- Case 2: The degree of trust $T(u,v)$ between the sensor nodes u and v can be referred to have a linear associations between security trust and ability trust function.
- Case 3: The variable degree of trust $T(u,v)$ between the sensor nodes u and v can be referred to as a key factor effecting the successive time interval (τ).
- *Negative trust* exists due to the behaviour of malicious nodes in MANETs.
- *Capacity trust* is the degree of trust $T(u,v)$ between the sensor nodes u and v can be referred to as a stand-alone efficiency.
- *Ability trust* is the participating sensor node capacity for message transmission and routing in order to establish trust relationship between the sensor nodes.
- *Safety trust* is the degree of trust $T(u,v)$ in the sensor nodes u that confirms the network behavior on the target node v.
- *Security trust* is the degree of trust $T(u,v)$ in the sensor nodes u prompt requests response, request accomplishment and data packets transfer that to the target node v.
- *Experience trust* states the past trusted sensor nodes behaviour in MANETs for establishing future trust.

3.5.2. Integrated calculation of trust model

Depending on the assumption made in Section 3.5.1, the degree of trust between the sensor nodes is estimated. For the first three cases, we use three different measurements to estimate the trust model. The expression for the calculation of the trust model is given below:

- Depending on the assumption in Case 1, the degree of trust between the sensor nodes u and v is $T_\tau(u,v)$, which is expressed as

$$T(u,v) : t \rightarrow R_0. \tag{13}$$

- Depending on the assumption in Case 2, the degree of trust between sensor nodes u and v is $T_\tau(u,v)$,

which is expressed as

$$T_t(u,v) = \varepsilon T_\tau^S(u,v) + (1-\varepsilon)T_\tau^A. \quad (14)$$

where $T_\tau^S(u,v)$ is the predicted trust value and T_τ^A is the ability trust evaluated value.ε is the modulus operator.

- Depending on the assumption in Case 2, the rate change of trust degree between sensor nodes u and v is $T_\tau(u,v)$, which is expressed as

$$\rho_\tau(u,v) = \frac{dT_\tau(u,v)}{d\tau}. \quad (15)$$

Additionally, the degree of trust between sensor nodes u and v is predicted using evaluation iteration formula that is expressed as

$$T_{\tau+1}(u,v) = e^{\rho_\tau(u,v)} T_\tau(u,v). \quad (16)$$

3.5.3. Trust computation inside the cluster

When a cluster head in ZRP sends a request across all sensor nodes lying inside its range, the need of computing the trust rate within the cluster between the cluster head and individual sensor nodes is necessary in such cases. The degree of trust is used by the sensor nodes to acknowledge the cluster head after the request is sent by the cluster head. Therefore the degree of trust $\vec{T}_{ch}$ insider a cluster is estimated as,

$$\vec{T}_{ch} = (\vec{T}_{ch,1}, \vec{T}_{ch,2}, \ldots, \vec{T}_{ch,n}) \quad (17)$$

Further, the degree of trust between cluster head and individual sensor nodes is calculated by,

$$\vec{T}_{ch,u} = \frac{\sum_{u=1}^{n-1} T(u,v)}{n-1} \quad (18)$$

where $\vec{T}_{ch,i}$ is the trust rate vector between the cluster head and an individual sensor node (u) inside the range of transmission.

3.5.4. Trust computation between head nodes

The degree of trust between the cluster head sensor nodes $CH(u)$ and $CH(v)$ is expressed as

$$T_{\tau+1}(u,v) = e^{\rho_\tau(u,v)} T_\tau(u,v). \quad (19)$$

This expression is quite important as the cluster head sensor node carries the data of its own cluster and other clusters.

3.5.5. Trust computation between clusters

The degree of trust between the clusters is estimated with the help of a differential equation and the estimation is carried out with the following equation:

$$\frac{T_{\tau+\Delta\tau}^I(u,v) - T_\tau^I(u,v)}{\Delta\tau} + \mu_0 T_\tau^I(u,v) = \mu_1 T_\tau^C(u,v) + \mu_2 T_\tau^M(u,v), \quad (20)$$

where $T^C(i,j)$ is the security trust value, $T^I(i,j)$ is the experience trust value and $T^M(i,j)$ is the negative trust value.

4. Performance metrics

The simulation is conducted using NS-2.34 simulator for the proposed trust mechanism for MANET architecture. ZRP routing protocol is used as an extension to provide support for the architecture of MANETs using the simulator. The ZRP routing protocol takes care of the entire routing process in MANETs. The network architecture is formed with 100 sensor nodes moving randomly in an area of 1000 m × 1000 m. Out of 100 sensor nodes, 10–50% of these sensor nodes are considered to be malicious that drops the transmitted packets at a dropping rate of 50–80%. Further, it is assumed that 30 source-destination sensor nodes pair makes direct communication with each other. Constant Bit Rate (CBR) traffic model is used for transmitting the packets between the source and destination nodes at a constant rate of four packets/second, and the destination nodes is assumed to have a pause time of one minute. The total simulation time of the proposed model takes place around 10.67 min. The sensor nodes joining the network is set with a trust level of 0.5 and the threshold trust value of each sensor node is set as 0.4 [33]. The parameters required for simulating the MANETs under proposed behaviour is given in Table 1.

In the proposed trust model, the packet drop ratio occurs at various percentages in selfish nodes (50% in MANETs) and this leads to collision or jamming of packets. The recommender system is targeted by blackhole attacks that provide dishonest recommendations for all the sensor nodes to drop the packets in MANET [34]. This attack allots false recommendation to the recommender system that degrades the trust value of estimated sensor node. It is assumed that 20% of the nodes recommended are of this type.

Table 1. Network configuration parameters.

Parameter	Value
Total number of sensor nodes	100
Area for simulation	1000 m × 1000 m
Mobility of sensor nodes	10 m/s
Range of transmission	250 m
Movement	Random Waypoint Model
MANET routing protocol	ZRP
Total number of source-destination node pairs	30
Capacity of transmission	2 Kbps
Traffic Type	CBR
Size of packet	512 Bytes
Simulation time	500 s
Deviation threshold	0.5
Threshold trust value	0.4
Pause time	10 s

5. Evaluation and discussions

The proposed method is evaluated using three QoS parameters including packet loss, network throughput and energy consumption. The proposed simulation is carried out in MANETs between the wireless nodes with misbehaving nodes. Three different cases are used for testing the proposed trust model in MANET architecture that evaluates the reliability of a sensor node, which is given below:

- Case 1: The packets are routed using ZRP routing algorithm and sensor nodes has no trust relationship with other sensor nodes;
- Case 2: The packets are routed using ZRP routing algorithm using packet forwarding rate and the sensor nodes have a trust relationship with other node;
- Case 3: The packets are routed using ZRP routing algorithm and the sensor nodes have proposed trust relationship with other node;

5.1. *Effect of malicious sensor nodes w.r.t performance metrics*

This subsection discusses the malicious sensor nodes effect on various performance metrics including packet loss, throughput and energy consumption in MANETs. The performance is tested under various percentages of malicious sensor nodes that ranges between 10% and 40%.

The results of overall throughput in the presence of malicious sensor nodes in MANETs is given in Figure 2. The graph shows a linear declination of throughput in the presence of misbehaving nodes. It is inferred from the graphs that Case 3 achieves higher throughput level, Case 2 has a moderate throughput and Case 1 records the least. This shows that the proposed method obtains higher overall throughput in the presence of ZRP routing protocol than the other methods.

Likewise, the results of packet loss in the presence of various percentages of malicious sensor nodes in MANETs is given in Figure 3. The result shows a linear inclination of packet loss rate in the presence of varying percentages of malicious sensor nodes. It is seen that the Case 1 has a higher packet loss rate, Case 2 has moderate packet loss rate and Case 3 records the least. The least packet loss ratio shows that the proposed method is effective even if the malicious sensor nodes varies dynamically.

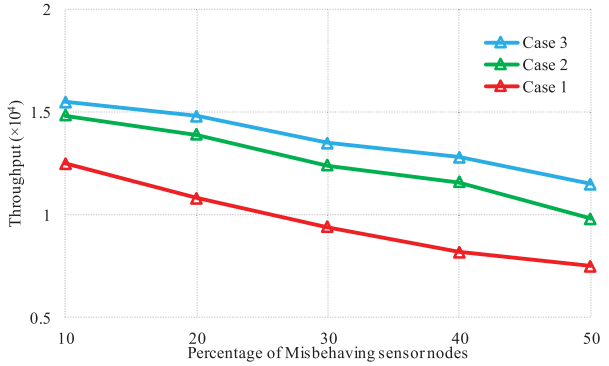

Figure 2. Overall throughput w.r.t various percentage of malicious sensor nodes.

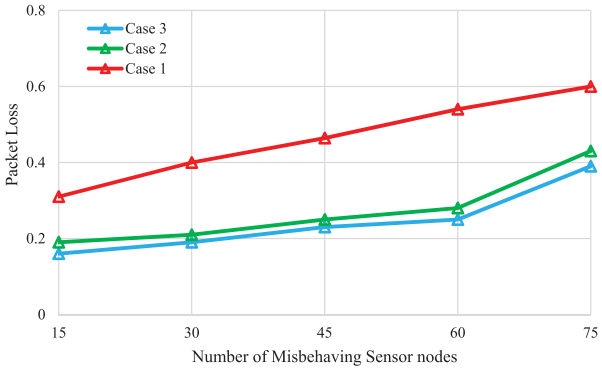

Figure 3. Packet loss w.r.t various percentage of malicious sensor nodes.

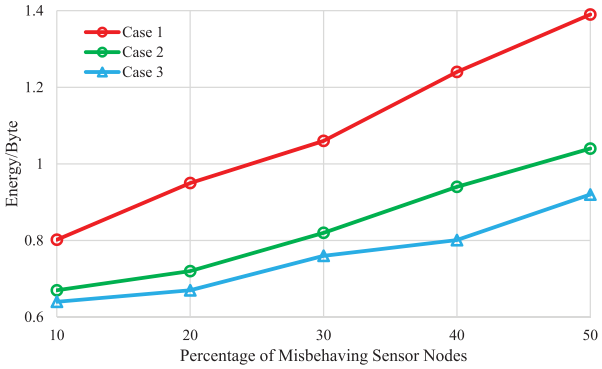

Figure 4. Consumption of energy w.r.t various percentage of malicious sensor nodes.

Finally, Figure 4 shows the consumption of energy due to the effects of varying percentages of malicious sensor nodes. The result shows that energy consumption is linearly increasing with varying percentages of malicious sensor nodes. It could be inferred from the results that Case 1 has a higher consumption of energy, Case 2 has moderate consumption of energy and Case 3 almost records the least energy consumption than other two cases.

Case 3 is tested further with Case 2 and Case 1 in terms of combined QoS metrics to measure the trust level of sensor nodes. It is evident from Figure 5 that Case 3 has a higher trust level than other two cases. The effect of energy consumption of sensor node trust value is measured and it is inferred that as the total number of sensor node interactions increases, the consumption of energy tends to increase and this reduces linearly the trust value.

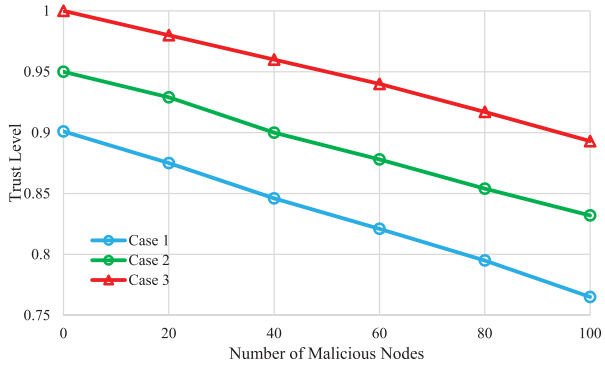

Figure 5. Trust level w.r.t various percentage of malicious sensor nodes.

5.2. Effect of malicious sensor nodes w.r.t trust level

This section discusses the trust level or the trustworthiness of corrupt, modest and noble sensor nodes during the coexistence of attacker nodes. In this evaluation, the Case 3 model is compared with Case 2 (refer Figure 6), since we consider trust level as an important factor to study the effectiveness of malicious sensor nodes.

The trust level of noble sensor nodes is shown in Figure 6(a). The total number of noble sensor nodes considered for evaluation is 30 and it increases as the total number of fortunate interactions with sensor nodes increases with time. The evaluated result shows that trust level for Case 3 is lesser than Case 2, since the Case 2 model evaluates the trust values during packet forwarding. On contrary, trust model in Case 3 estimates all the factors associated in network for finding the trust value of calculated sensor node.

The trust level of modest sensor nodes is shown in Figure 6(b). The total number of noble sensor nodes considered for evaluation is 17 and it increases as the total number of fortunate interactions with sensor nodes increases with time. It is seen that trust level obtained through modest sensor nodes is lesser than the trust level obtained through noble sensor nodes (Figure 6(a)).

The trust level of corrupt sensor nodes is shown in Figure 6(c). The total number of noble sensor nodes considered for evaluation is 13 and it is noticeable that the trust level of corrupt sensor nodes is recorded to be the least. However, the result shows that the Case 2 has higher trust level than Case 3 as all the corrupt nodes conduct attacks on other nodes based on the available energy resources as well as the sensor node intimacy is recorded to be the lowest.

5.3. Effect of decision making w.r.t trust level

For evaluating the identification of message, the proposed system uses two metrics to test its performance including Missed Detection Rate (MDR) and

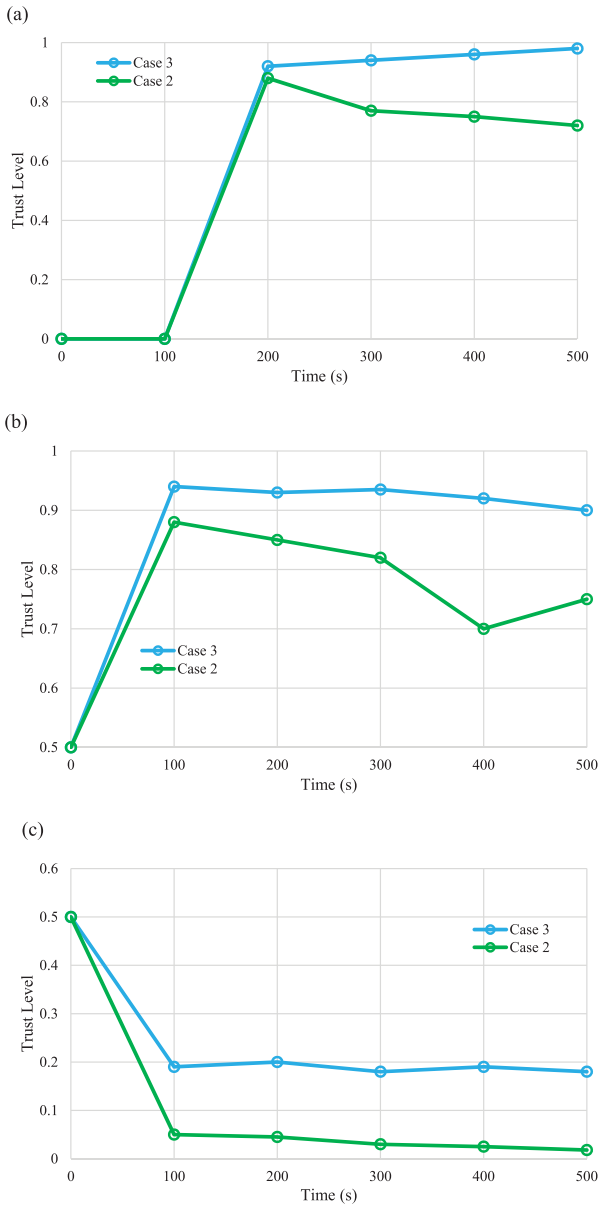

Figure 6. (a) Trust level of noble sensor nodes. (b) Trust level of modest sensor nodes and (c): Trust level of corrupt sensor nodes.

False Alarm Rate (FAR), which is given in following equations,

$$\text{MDR} = \frac{N_{mis}}{N} \text{ and FAR} = \frac{N_f}{N_i},$$

where N_f is the number of false recognized by the method, which is recognized as true packets, N_i is the number of packets recognized by the method and N_{mis} is the Number of true packets recognized by the method, which is recognized as false packets and N is the number of true packets recognized by the method.

Figure 7 shows the comparison of FAR between different cases. The result shows that Case 3 has lower FAR than the other two cases. Similarly, the MDR of Case 3 is lesser than the other two cases (Figure 8), which indicates that Case 3 is reliable than the other two cases. This shows that the proposed method is effective in MANETs.

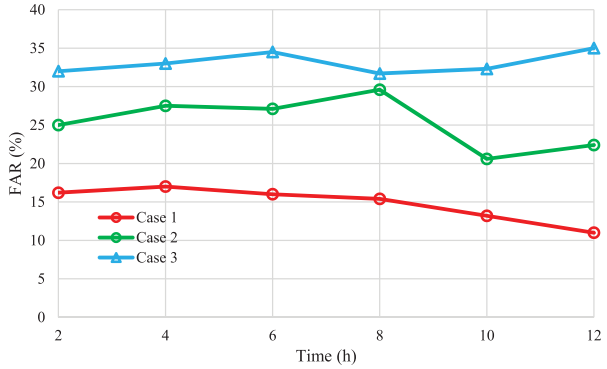

Figure 7. FAR between different cases.

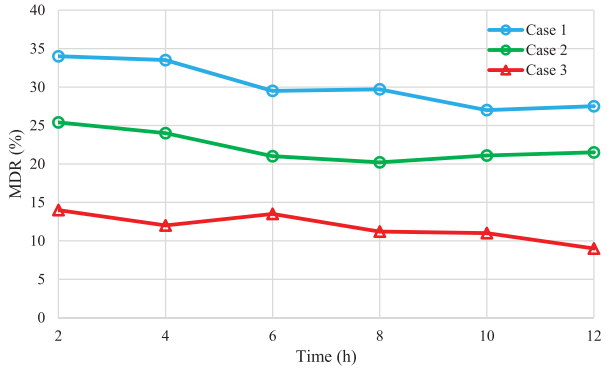

Figure 8. MDR between different cases.

6. Conclusions and future work

In this paper, we propose a new trust model and analysed the effectiveness of how a secured node can be routed inside MANETs through QoS metrics. This trust model makes use of direct, indirect and mutual trust values between the sensor nodes to reflect the behaviour of sensor nodes. The combination of all these trust values helps to evaluate the trust level of independent sensor nodes and provides the recognition of an abnormal node in the network. The trust level for all the sensor nodes is evaluated using QoS metrics that provides an accurate recommendation for forwarding the packets, thereby it reduces the packet drops. The performance evaluation of the proposed trust model obtains reduced packet loss, increased overall network throughput and reduced energy consumption in the presence of a varying percentage of malicious black-hole nodes. Finally, it could be concluded that the proposed trust method obtains improved overall network performance.

Their results show that the proposed algorithm can outperform the existing single trust-based model by effectively filtering out malicious nodes conducting various attacks, as well as penalizing attackers with loss of reputation, which may lead to user satisfaction. In addition, their model is efficient, with linear run time complexity, achieving a close-to-optimal solution.

Disclosure statement

The learner could easily grasp the Qos, Black Hole attacks in MANET using this framework. The Analysis report would really help to upcoming researchers in this field.

References

[1] Andel TR, Yasinsac A. Surveying security analysis techniques in MANET routing protocols. IEEE Commun Surv Tutorials. 2007;9(4):70–84.
[2] Walikar GA, Biradar RC. A survey on hybrid routing mechanisms in mobile ad hoc networks. J Netw Comput Appl. 2017;77:48–63.
[3] Gulati MK, Kumar K. A review of qos routing protocols in manets. In Computer Communication and Informatics (ICCCI), 2013 International Conference on. IEEE; 2013, January. pp. 1–6.
[4] Cordasco J, Wetzel S. Cryptographic versus trust-based methods for MA-NET routing security. Electron Notes Theor Comput Sci. 2008;197(2):131–140.
[5] Cordasco J, Wetzel S. Cryptographic versus trust-based methods for MANET routing security. Electron Notes Theor Comput Sci. 2008;197(2):131–140.
[6] Singh S. A review of trust management for mobile ad hoc networks. In: Singh D, editor. Routing protocols and architectural solutions for optimal wireless networks and se-curity. Hershey, PA: IGI Global; 2017. p. 142–154.
[7] Michiardi P, Molva R. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In: Advanced communications and multimedia security. Boston, MA: Springer; 2002. p. 107–121.
[8] Shabut AM, Dahal K, Awan I. Enhancing dynamic recommender selection using multiple rules for trust and Reputation Models in MANETs. In Tools with Artificial Intelligence (ICTAI), 2013 IEEE 25th International Conference on; IEEE; 2013, November. pp. 654–660.
[9] Katsaros D, Dimokas N, Tassiulas L. Social network analysis concepts in the design of wireless ad hoc network protocols. IEEE Netw. 2010;24(6):23–29.
[10] Zhao X, You Z, Zhao Z, et al. Availability based trust model of clusters for MANET. In Service Systems and Service Management (ICSSSM), 2010 7th International Conference on. IEEE; 2010, June. p. 1–6.
[11] Blaze M, Feigenbaum J, Ioannidis J, et al. The role of trust management in distributed systems security. In: Vitek J, Jensen CD, editors. Secure internet programming. Berlin, Heidelberg: Springer; 1999. p. 185–210.
[12] Cho JH, Swami A, Chen R. Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks. J Netw Comput Appl. 2012;35(3):1001–1012.
[13] Xia H, Jia Z, Ju L, et al. A subjective trust management model with multiple decision factors for MANET based on AHP and fuzzy logic rules. In Green Computing and Communications (GreenCom), 2011 IEEE/ACM International Conference on. IEEE; 2011 August. pp. 124–130.
[14] Xu G, Yan Z. A survey on trust evaluation in mobile ad hoc networks. In Proceedings of the 9th EAI International Conference on Mobile Multimedia CommunicationsICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering); 2016 June. pp. 140-148.

[15] Chen D, Chang G, Sun D, et al. TRM-IoT: A trust management model based on fuzzy reputation for internet of things. Computer Science and Information Systems. 2011;8(4):1207–1228.
[16] Pirzada AA, McDonald C. Trust establishment in pure ad-hoc networks. Wirel Pers Commun. 2006;37(1–2): 139–168.
[17] Chen R, Guo J, Bao F. Trust management for SOA-based IoT and its application to service composition. IEEE Transactions on Services Computing. 2016;9(3):482–495.
[18] Velloso PB, Laufer RP, Cunha DDO, et al. Trust management in mobile ad hoc networks using a scalable maturity-based model. IEEE Trans Netw Serv Manage. 2010;7(3):172–185.
[19] Agrawal A, Verma AK. A review & impact of Trust Schemes in MANET. In Proceedings of the International Conference on Advances in Information Communication Technology & Computing ACM; 2016, August. p. 26.
[20] Li B, Liao L, Leung H, et al. PHAT: A preference and honesty aware trust model for web services. IEEE Trans Netw Serv Manage. 2014;11(3):363–375.
[21] Mehdi M, Bouguila N, Bentahar J. Trust and reputation of web services through QoS correlation lens. IEEE Trans Serv Comput. 2016; (1):1–1.
[22] Yang Y, Liu R, Chen Y, et al. Normal cloud model-based algorithm for multi-attribute trusted cloud service selection. IEEE Access. 2018;6:37644–37652.
[23] Mao C, Lin R, Xu C, et al. Towards a trust prediction framework for cloud services based on PSO-driven neural network. IEEE Access. 2017;5:2187–2199.
[24] Li W, Zhang P, Leung H, et al. A novel QoS prediction approach for cloud services using Bayesian network model. IEEE Access. 2018;6:1391–1406.
[25] Jia C, Xie L, Gan X, et al. A trust and reputation model considering overall peer consulting distribution. IEEE Trans Syst Man Cyber Syst Hum. 2012;42(1): 164–177.
[26] Shen H, Lin Y, Li Z. Refining reputation to truly select high-QoS servers in peer-to-peer networks. IEEE Trans Parallel Distrib Syst. 2013;24(12):2439–2450.
[27] Li J, Bai Y, Zaman N, et al. A decentralized trustworthy context and QoS-aware service discovery framework for the Internet of things. IEEE Access. 2017;5: 19154–19166.
[28] Bao F, Chen R, Chang M, et al. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE Trans Netw Serv Manage. 2012;9(2): 169–183.
[29] Lin K, Rodrigues JJ, Ge H, et al. Energy efficiency QoS assurance routing in wireless multimedia sensor networks. IEEE Syst J. 2011;5(4):495–505.
[30] Moustafa A, Zhang M, Bai Q. Trustworthy stigmergic service composition and adaptation in decentralized environments. IEEE Trans Serv Comput. 2016;9(2):317–329.
[31] Ch RM. M-LionWhale: multi-objective optimization model for secure routing in mobile Ad-hoc network. IET Commun. 2018;12(12):1406–1415.
[32] Basurra SS, De Vos M, Padget J, et al. Energy efficient zone based routing protocol for MANETs. Ad Hoc Netw. (2015);25:16–37.
[33] Li R, Li J, Liu P, et al. A novel hybrid trust management framework for MANETs. In 2009 29th IEEE International Conference on Distributed Computing Systems Workshops. IEEE; 2009 June. p. 251–256.
[34] Islam MH, Khan AA.. Detection of dishonest trust recommendations in mobile ad hoc networks. In Computing, Communication and Networking Technologies (ICCCNT), 2014 International Conference onIEEE. 2014 July. p. 1–7.